IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of: *Gross et. al.*	)	
	)	Examiner: Lamont Spooner
Serial No.: 10/723,370	)	
	)	
Filed: *November 24, 2003 as a continuation of serial no. 09/014,414 filed 1/27/98*	)	
	)	
	)	
For: *Email Text Checker System and Method*	)	

-

Appeal Brief filed under 37 C.F.R. § 1.192

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Per 37 C.F.R. § 41.37 Appellants submit the present Appeal Brief in furtherance of the Notice of Appeal filed in this case on March 7, 2008.

Please charge any fees, including for a one month extension of time, in accordance with the accompanying Transmittal letter. A short introduction of the prosecution history is first presented. This brief also contains the following sections as required by 37 C.F.R. § 41.37 and MPEP § 1206:

BRIEF INTRODUCTION AND REVIEW OF PROSECUTION HISTORY

This brief is presented in support of the Notice of Appeal filed for application serial no. 10/723,370 filed March 7, 2008. The present application was filed on November 24, 2003 and claims priority to parent application serial no. 09/014,414 filed January 31, 1998, now U.S. Patent No. 6,782,510.

Originally filed claims 83 – 87 and 92, 96 were rejected under §102 in light of Cohen (U.S. Patent No. 5,796,948) in a first Office Action mailed June 9, 2006.[1] Claims 88, 89 and 97 were rejected under §103 based on Cohen taken with Ishikawa (U.S. Patent No. 5,812,863). Claims 90, 91, 93, 98 and 99 were rejected under §103 based on Cohen taken with Russell-Falla et al. (U.S. Patent No. 6,675,162). Claims 94, 95 and 100 – 103 were rejected under §103 based on Cohen taken with Rayson et al. (U.S. Patent No. 5,761,689).

On September 14 2006 Applicant filed an Amendment A to the first Office Action, in which the rejection based on Cohen was traversed based on the fact that in such reference the user cannot transmit a message through the system if it contains content that has triggered the profanity filter. A discussion of Ishikawa, Russell-Falla and Rayson was also presented for the obviousness arguments.

A second final Office action was mailed on November 6, 2006. The Examiner argued that Cohen inherently taught the aforementioned limitation, and on this basis maintained the §102 rejections. The Examiner further maintained the §103 rejections based on Ishikawa, Russell-Falla and Rayson.

An Amendment B was filed after Final on December 4, 2006. The Applicant pointed out that the Patent Office had not explained or shown anywhere how the Cohen

[1] The claims were also rejected under provisional double patenting, but this issue has been resolved and is not part of this appeal.

reference could "inherently" perform the steps of claim 83. The distinctions over Ishikawa, Russell-Falla and Rayson were again repeated.

In an Advisory Action mailed January 10, 2007, the Examiner elected not to enter Amendment B because he claimed it raised new issues. For this reason Applicant filed an RCE on February 6, 2007 asking for entry of the December 4 2006 amendment.

The Examiner maintained the rejection of the claims again on April 20, 2007, based on an argument that somehow "claim 1" did not in fact contain the limitation argued by the Applicant in the Amendment as the distinction over Cohen et al. See Office Action pages 2 – 3. The Applicant, in both telephone and written communications dated July 27, 2007, earnestly requested that the Examiner review and re-issue the Office Action given the blatant error, *since there was no claim 1 pending at the time, and claim 83 did in fact contain the limitation in question.*

No response was ever given by the Examiner, so the Applicant was forced to file an Amendment C on October 10, 2007, without the benefit of a proper Office Action. The Applicant further emphasized the distinction over Cohen, noting that claim 83 now required that the system cause the email message to be transmitted.

The Examiner then newly cited Bradshaw in a final Office Action dated December 7, 2007 as somehow curing the aforementioned deficiency of Cohen et al, thereby rendering claim 83 obvious. The Examiner contends that in the Bradshaw reference, an author of an email message can cause such message to be transmitted even if it falls within a language filter. See 12/7/07 Office Action, page 6.
The rejections of the other claims (88, 89, 97; 90, 91, 93, 98, 99; and 94, 95 and 100-103) based on Cohen taken with Ishikawa, Russell-Falla and Rayson respectively were again repeated.

In a Response D after Final, the Applicant traversed the combination of Cohen et al. and Bradshaw, primarily on the grounds that the latter does not in fact operate the way the Examiner believed, and hence could not cure the deficiencies of Cohen. Because the Examiner rejected these arguments again in an Advisory Action mailed March 3, 2008, Applicant filed the present appeal.

I. REAL PARTY IN INTEREST

John Nicholas Gross, residing at 3883 18th Street, San Francisco, CA 94114, and Anthony A. Gross residing at 213 Commodore Drive, Richmond, CA 94804.

II. RELATED APPEALS AND INTERFERENCES

There are no other appeals, interferences or judicial proceedings known to Appellant, Appellant's legal representative, or the Assignee of the present application which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 83 - 103 are pending and all stand rejected under §103. Claims 83, 93, 94, 95, 96, 98, 100 and 102 are independent. A complete copy of the pending claims is provided in Appendix A.

IV. STATUS OF AMENDMENTS

There are no non-entered amendments to the claims.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 83

Independent claim 83 covers:[2]

A method of permitting an author of an electronic mail (email) message to check text content using an electronic text editor program operating on a computing system (FIG. 1; document 40, computing system 10, word checker 30; FIG. 2, page 7, l. 23 – page 8, l. 11; page 12, ll. 3 – 7), the method comprising:

(a) selecting a language filter for checking words in the email message, which language filter includes a first set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; and (FIG. 1, dictionaries 50, 51; page 8, ll. 12 – 20; page 9, ll. 11 – 26; page 10, ll. 4 – 25; page 12, ll. 8 – 25; page 15, ll. 1 - 24)

(b) receiving input words entered by the author as text for the email message; (FIG. 2, steps 210, 215; page 7, l. 24 - page 8, l. 2)

(c) inspecting said input words to determine if they fall within said language filter; (FIG. 2, steps 235; page 7, l. 24 - page 8, l. 3 – page 10, l. 25)

(d) alerting the author when one or more of said input words fall within said language filter; (FIG. 2, step 240; page 11, ll. 10 – 17);

(e) permitting the author to change words within the email message after step (d) and before the email message is transmitted to said intended recipient; and (FIG. 2, step 245; page 11, ll. 18 – 24)

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter. (See FIG. 2 – "override" condition between steps 245/250; page 11, ll. 25 – page 12, l.2)

[2] In the interest of efficiency and clarity Applicant has not identified every single aspect of the disclosure which may pertain to the claimed limitations.

Independent claim 93 covers:

A method of permitting an author of an electronic mail (email) message to check text content using an electronic text editor program operating on a computing system, (FIG. 1; document 40, computing system 10, word checker 30; FIG. 2, page 7, l. 23 – page 8, l. 11; page 12, ll. 3 – 7) the method comprising:

(a) selecting a language filter for checking words in the email message, which language filter can be configured to control dissemination of content to an intended recipient of the email message; (FIG. 1, dictionaries 50, 51; page 8, ll. 12 – 20; page 9, ll. 11 – 26; page 10, ll. 4 – 25; page 12, ll. 8 – 25; page 15, ll. 1 - 24) and

(b) setting a sensitivity threshold provided by the author to also be used in connection with checking appropriateness of content included in the email message; (page 10, ll. 21 – 25; page 11, ll.25 - 27)

(c) retrieving input words entered by the author as text for the email message; (FIG. 2, steps 210, 215; page 7, l. 24 - page 8, l. 2)

(d) inspecting said input words to determine if they fall within said language filter; (FIG. 2, steps 235; page 7, l. 24 - page 8, l. 3 – page 10, l. 25)

(e) providing a warning to the author if an input word falls within said language filter and said sensitivity threshold is exceeded; (FIG. 2, step 240; page 11, ll. 10 – 17);

(f) permitting the author to change words within the email message after a warning is made and before the email message is transmitted to said intended recipient; (FIG. 2, step 245; page 11, ll. 18 – 24)

and

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter. (See FIG. 2 – "override" condition between steps 245/250; page 11, ll. 25 – page 12, l.2)

Independent claim 94 covers:

A method of checking text content of an email message using an electronic text editor program operating on a computing system (FIG. 1; document 40, computing system 10, word checker 30; FIG. 2, page 7, l. 23 – page 8, l. 11; page 12, ll. 3 – 7) the method comprising:

(a) selecting a language filter for checking words in the email message, which language filter includes a set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; (FIG. 1, dictionaries 50, 51; page 8, ll. 12 – 20; page 9, ll. 11 – 26; page 10, ll. 4 – 25; page 12, ll. 8 – 25; page 15, ll. 1 - 24) and

(b) receiving an input word entered by the author as text for the email message; (FIG. 2, steps 210, 215; page 7, l. 24 - page 8, l. 2)

(c) inspecting said input word substantially immediate in time after it is entered to determine if it falls within said language filter; (FIG. 2, steps 235; page 7, l. 24 - page 8, l. 3 – page 10, l. 25; also, page 13, l. 14 – page 14, l. 7 with respect to time element)

(d) providing a warning to the author when said input word is determined to fall within said language filter; (FIG. 2, step 240; page 11, ll. 10 – 17);

(e) permitting the author to change said input word within the email message after a warning is made and before the email message is transmitted to said intended recipient; and (FIG. 2, step 245; page 11, ll. 18 – 24)

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if said input word falls within said language filter. (See FIG. 2 – "override" condition between steps 245/250; page 11, ll. 25 – page 12, l.2)

Independent claim 95 covers:

A method of checking text content of an email message using an electronic text editor program operating on a computing system (FIG. 1; document 40, computing system 10, word checker 30; FIG. 2, page 7, l. 23 – page 8, l. 11; page 12, ll. 3 – 7) the method comprising:

(a) selecting a language filter for checking words in the email message, which language filter includes a set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; (FIG. 1, dictionaries 50, 51; page 8, ll. 12 – 20; page 9, ll. 11 – 26; page 10, ll. 4 – 25; page 12, ll. 8 – 25; page 15, ll. 1 - 24) and

(b) receiving input words entered by the author as text for the email message; (FIG. 2, steps 210, 215; page 7, l. 24 - page 8, l. 2)

(c) inspecting said input words during idle periods when the author is not interacting with said electronic text editor program to determine if such input words fall within said language filter; (FIG. 2, steps 235; page 7, l. 24 - page 8, l. 3 – page 10, l. 25; also, page 13, ll. 5 - 13 with respect to idle periods limitation)

(d) providing a warning to the author when one or more of said input words are determined to fall within said language filter; (FIG. 2, step 240; page 11, ll. 10 – 17);

(e) permitting the author to change words within the email message after a warning is made and before the email message is transmitted to said intended recipient; and (FIG. 2, step 245; page 11, ll. 18 – 24)

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter. (See FIG. 2 – "override" condition between steps 245/250; page 11, ll. 25 – page 12, l.2)

Independent claim 96 covers:

A computer program for checking text content of an email message using an electronic text editor program operating on a computing system, (FIG. 1; document 40, computing system 10, word checker 30; FIG. 2, page 7, l. 23 – page 8, l. 11; page 12, ll. 3 – 7) comprising:

a language filter for checking words in the email message, which language filter is an electronic dictionary which includes a set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; (FIG. 1, dictionaries 50, 51; page 8, ll. 12 – 20; page 9, ll. 11 – 26; page 10, ll. 4 – 25; page 12, ll. 8 – 25; page 15, ll. 1 - 24) and

and

a content checking routine which is adapted for: (word checker 30)

i) receiving input words entered by the author as text for the email message; (FIG. 2, steps 210, 215; page 7, l. 24 - page 8, l. 2)

ii) inspecting said input words to determine if they fall within said language filter; (FIG. 2, steps 235; page 7, l. 24 - page 8, l. 3 – page 10, l. 25)

iii) generating an alert to the author when one or more of said input words fall within said language filter; (FIG. 2, step 240; page 11, ll. 10 – 17);

iv) permitting the author to change words within the email message after an alert is generated and before the email message is transmitted to said intended recipient; and (FIG. 2, step 245; page 11, ll. 18 – 24)

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter. (See FIG. 2 – "override" condition between steps 245/250; page 11, ll. 25 – page 12, l.2)

Independent claim 98 covers:

A computer program for permitting an author of an electronic mail (email) message to check text content, comprising: (FIG. 1; document 40, computing system 10, word checker 30; FIG. 2, page 7, l. 23 – page 8, l. 11; page 12, ll. 3 – 7)

a language filter for checking words in the email message, which language filter can be configured to control dissemination of content to an intended recipient of the email message; (FIG. 1, dictionaries 50, 51; page 8, ll. 12 – 20; page 9, ll. 11 – 26; page 10, ll. 4 – 25; page 12, ll. 8 – 25; page 15, ll. 1 - 24) and

a content checking routine which is adapted for: (word checker 30)

i) setting a sensitivity threshold provided by the author to also be used in connection with checking appropriateness of content included in the email message; (page 10, ll. 21 – 25; page 11, ll.25 - 27)

ii) retrieving input words entered by the author as text for the email message; (FIG. 2, steps 210, 215; page 7, l. 24 - page 8, l. 2)

iii) inspecting said input words to determine if they fall within said language filter; (FIG. 2, steps 235; page 7, l. 24 - page 8, l. 3 – page 10, l. 25)

iv) providing a warning to the author if an input word falls within said language filter and said sensitivity threshold is exceeded; (FIG. 2, step 240; page 11, ll. 10 – 17);

v) permitting the author to change words within the email message after a warning is made and before the email message is transmitted to said intended recipient; (FIG. 2, step 245; page 11, ll. 18 – 24) and

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter. (See FIG. 2 – "override" condition between steps 245/250; page 11, ll. 25 – page 12, l.2)

Independent claim 100 covers:

A computer program operating on a computing system for checking text content of an email message (FIG. 1; document 40, computing system 10, word checker 30; FIG. 2, page 7, l. 23 – page 8, l. 11; page 12, ll. 3 – 7) comprising:

a language filter for checking words in the email message, which language filter includes a set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; (FIG. 1, dictionaries 50, 51; page 8, ll. 12 – 20; page 9, ll. 11 – 26; page 10, ll. 4 – 25; page 12, ll. 8 – 25; page 15, ll. 1 - 24)and

a content checking routine (word checker 30) adapted for:

i) receiving an input word entered by the author as text for the email message; (FIG. 2, steps 210, 215; page 7, l. 24 - page 8, l. 2)

ii) inspecting said input word substantially immediate in time after it is entered to determine if it falls within said language filter; (FIG. 2, steps 235; page 7, l. 24 - page 8, l. 3 – page 10, l. 25; also, page 13, l. 14 – page 14, l. 7 with respect to time element)

iii) providing a warning to the author when said input word is determined to fall within said language filter; (FIG. 2, step 240; page 11, ll. 10 – 17);

iv) permitting the author to change said input word within the email message after a warning is made and before the email message is transmitted to said intended recipient; and (FIG. 2, step 245; page 11, ll. 18 – 24)

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter. (See FIG. 2 – "override" condition between steps 245/250; page 11, ll. 25 – page 12, l.2)

Independent claim 102 covers:

A computer program operating on a computing system for checking text content of an email message (FIG. 1; document 40, computing system 10, word checker 30; FIG. 2, page 7, l. 23 – page 8, l. 11; page 12, ll. 3 – 7) comprising:

a language filter for checking words in the email message, which language filter includes a set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; (FIG. 1, dictionaries 50, 51; page 8, ll. 12 – 20; page 9, ll. 11 – 26; page 10, ll. 4 – 25; page 12, ll. 8 – 25; page 15, ll. 1 - 24) and

a content checking routine (word checker 30) adapted for:

i) receiving input words entered by the author as text for the email message; (FIG. 2, steps 210, 215; page 7, l. 24 - page 8, l. 2)

ii) inspecting said input words during idle periods when the author is not interacting with said electronic text editor program to determine if such input words fall within said language filter; (FIG. 2, steps 235; page 7, l. 24 - page 8, l. 3 – page 10, l. 25; also, page 13, ll. 5 - 13 with respect to idle periods limitation)

iii) providing a warning to the author when one or more of said input words are determined to fall within said language filter; (FIG. 2, step 240; page 11, ll. 10 – 17);

iv) permitting the author to change words within the email message after a warning is made and before the email message is transmitted to said intended recipient; and (FIG. 2, step 245; page 11, ll. 18 – 24)

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter. (See FIG. 2 – "override" condition between steps 245/250; page 11, ll. 25 – page 12, l.2)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The issues presented for appeal are:

1. whether independent claims 83, 96 and dependent claims 84 – 87, 92 are unpatentable under § 103 in light of Cohen et al (U.S. Patent No. 5,796,948) taken with Bradshaw et al. (U.S. Patent No. 5,835,722)
2. whether claims 88, 89 and 97 (depending from claims 83, 96 respectively) are further unpatentable under § 103 in light of the above taken with Ishikawa (U.S. Patent No 5,812,863)
3. whether independent claim 98 (and claim 99 depending therefrom) and claims 90, 91, 93 (depending from claim 83) are further unpatentable under § 103 in light of the above taken with Russell-Falla et al. (U.S. Patent No 6,671,162)
4. whether independent claim 94 (and claim 95 depending therefrom) and Independent claims 100, 102 (and claims 101, 103 depending from these claims respectively) are further unpatentable under § 103 in light of the above taken with Rayson et al. (U.S. Patent No 5,761,689)

VII. GROUPING OF CLAIMS

Except where noted below, the claims do not stand or fall together because they are directed to different facets of the present inventions and/or are more particularly directed to specific features of such inventions. A detailed discussion of such differences is given below.

VIII. ARGUMENT

The present claims relate, in general, to the field of content filtering and assisting authors to ensure that their content is in compliance with various language/content filters that may be applicable for a particular electronic document. The claims of the present application all recite the use of methods and programs that are relevant to the field of email/messaging, which is notoriously fraught with problems of inadvertent communications of inappropriate material.

The prior art cited by the Examiner is characterized by rather rigid and unforgiving language filter tools which are not designed to be "author" friendly. As is apparent, these systems are primarily focused on preventing users from circumventing language and access filters, and not on helping authors to craft more appropriate documents for particular audiences. Thus as a practical matter the primary prior art references (Cohen et al., Bradshaw et al.) do not discuss the type of situation or problem presented in the current disclosure. In fact, as is explained below, by insisting that users be deprived of information within language filters, or subjecting them to rigid rules, these disclosures teach away from the kind of approach embodied in the present claims.

1. Discussions of rejection of independent claims 83, 96 and dependent claims 84 – 87, 92 as unpatentable under § 103 in light of Cohen et al (U.S. Patent No. 5,796,948) taken with Bradshaw et al. (U.S. Patent No. 5,835,722)

The Examiner cited to the combination of Cohen and Bradshaw et al. above as making the above claims obvious. In the prior Office Actions the Examiner conceded that Cohen did not teach limitation (d) of claim 83, namely:[3]

> ....wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter.

In other words, consistent with the discussion above, the author of the email message is allowed to send the email even if it otherwise falls within a language filter.

[3] No admission or inference should be drawn from the present record as to the nature or scope of other claims issued or pending to the Applicant to such subject matter which do not specifically recite the language at issue here for the present claims.

The benefit here, of course, is that such type of system is more author/user-friendly, and allows for situations in which inadvertent tripping of a language filter can still be over-rode by the author because, for example, the author may decide the context for the word is in fact appropriate, or the recipient is exempt from a particular policy, etc.

In contrast, Cohen specifically mandates that the user must remove/edit the content (words) of the message before it can be actually transmitted to an intended recipient:

"....At step 520 the user edits said selected file 480, **therein "editing out" profane language** that is captured in brackets (see steps 270 and 280, FIG. 2). Said brackets thereby serve the user in locating and eliminating the profane language that had previously prevented the message from being sent. At step 530, **the edited message may be filed** (step 90, FIG. 1) and the user given the option to re-send said message (step 120, FIG. 1) (emphasis added).

This can be confirmed from examining block 520 in FIG. 5; EVERY offending message in Cohen MUST be edited to pass the profanity filter or it will not be transmitted. In col. 4, ll. 66 – 67 Cohen further states: "...the user may elect to edit the undeliverable message before attempting to re-send it..." The use of the terms "undeliverable" and "attempting" clearly indicate that the uncertainty associated with actually delivering the message exists until the user conforms the message.

While the user in Cohen is alerted to the offending text, and allowed to modify the message, the goals and objectives of Cohen make clear that it is not intended to assist authors by checking the content of their messages and alerting them to inappropriate choices so that they can learn and experiment with more appropriate language. Instead there is a "Big Brother" approach in which only the system administrator is allowed to determine what is or is not acceptable for a particular audience. There is no allowance for bypassing the system based on an individual author's choice.

Because of this omission in Cohen, the Examiner now relies on Bradshaw et al. Nonetheless this reference does not appear in fact to teach the above limitation, so as an initial point the present argument notes that the rejection is improper for this reason. The Examiner's characterization of Bradshaw is given on page 6 of the December 7, 2007 Office Action:

However, Bradshaw teaches the above lacking limitation, wherein the author ...even if words... (C.2 lines 57-67-screen production of email, C.3 lines 10-34, C.4 lines 18-21, Bradshaw explicitly teaches giving supervisory control to the screening of content to a user, libraries, and sent content, including a supervisor, see abstract. Thus, the user/supervisor may screen for content, and possess the ability to send the content, see C.4 lines 18-21 which discuss offensive content sent via email, as within the supervisory powers of the author, C.9 lines 34-36 allow the user content screening, yet allow the user to continue with the transmission of the content with only a warning).

This characterization of Bradshaw is plainly incorrect and not supported by the passages cited by the Examiner. Bradshaw is basically also a "blocking" system like Cohen with no allowance for users to bypass the controls.

Bradshaw purports to prevent children/students from accessing or creating offensive materials. As an initial matter, to the extent the Examiner believes that Bradshaw indicates that *such* persons (as "authors" of queries/documents) are able to send/control content, this is demonstrably wrong. Every passage cited by the Examiner confirms that a *supervisor*, usually an adult, is in control and screens what content is permitted to be sent/received.

To wit at col. 2, ll. 57 – 67 (cited by the Examiner) it indicates that the system therein:

> ...*allows interaction and control by a supervising adult* over what is screened..the comprehensive approach of the present invention not only blocks access to certain sites but also blocks the production of documents, E-mail, etc.... (emphasis added)

Note the specific indication that a "supervising" adult is necessary to screen content. In col. 3, ll. 18 – 21 also cited by the Examiner, it is further explained that:

> "E-mail can be controlled by prohibiting e-mail to certain addresses, *and enabling a supervisory adult* to monitor incoming and outgoing E-email." (emphasis added)

Thus this repeats the express requirement that a "supervisory" adult is required to control the email.

The other passages by the Examiner are all consistent: the child/student author is not allowed to send/receive materials on their own, or to bypass the blocking software. See e.g. col. 4, ll. 18 – 21 cited by the Examiner:

> "…If offensive material is sent or received via E-mail, the *parent* can review the E-mail activity, block transmissions to the offensive site…."

Applicant submits that it could not be clearer that Bradshaw does NOT permit authors to bypass the security/blocking software. As explained at col. 9, ll. 1 – 5, when users/authors attempt to circumvent the blocking routine, they are left with "…two choices (1) to call a supervisor to disable the system with a password or (2) reboot the computer…."

In the Office Action the Examiner *appears* to suggest nonetheless that the supervisor can qualify as the "author" of the content either through their own document composition, or merely because he/she determines *whether* to allow the content by the other users to be sent or not. This rejection is traversed on two different grounds.

First nothing in Bradshaw suggests that a supervisor can compose a document and successfully evade the "X-stop" blocking monitor. In fact, in the section cited by the Examiner it suggests that the supervisor's option is limited to *closing* the application.

"…A supervisor can avoid the monitoring of the computer by closing X-Stop." See col. 9, ll. 7 – 8.

However, in such instances where the monitor is disabled and the Supervisor then composes an email message, it clearly *cannot* meet the language of the present claims because the monitor is not checking anything.

Second, the supervisor does not become an "author" simply because they can *send* the message composed by a third party, such as a child/student. This is an unsupportable definition for the term "author" and the Examiner has cited no support for such an unreasonable interpretation.

Furthermore claim 83 specifies that it is a method of "…permitting an *author* of an electronic mail (email) message *to check content* using an electronic text editor program…" The supervisor in the Bradshaw system does not meet this requirement, since he/she does not contribute to the content of the message, or "check" the content. In the instance where the Supervisor is involved, the document in question has *already* been checked.

Third, the Examiner cites to col. 9, ll. 34 – 36 of Bradshaw as suggesting that it allows the user "...to continue with the transmission of the content with only a warning." This is a misinterpretation of what Bradshaw actually teaches. To ensure that there is a proper understanding of Bradshaw, Applicant reproduces the actual section of the disclosure below:

> ....Alternate blocking routines may include routines *that prevent transmission of prohibited words by* deleting them from the keyboard queue, clipboard, etc., without interfering with further operation of the computer, intervening with only a temporary warning screen, or audible warning. (emphasis added)

The correct grammatical parsing of this sentence compels the conclusion that Bradshaw nonetheless always prevents transmission of prohibited words, although this is accompanied with different side effects. In the first technique, their transmission is blocked by "deleting" them from the keyboard queue. In a second technique they are blocked but *without interfering further operation* of the computer. In a third instance they are blocked and accompanied by a *temporary warning screen.* But the usage of the terms "...deleting...without interfering...intervening.." etc. in the sentence make it clear that the action is nevertheless still accompanied by the fact that the prohibited words are not transmitted. This section of Bradshaw is merely suggesting other techniques than the harsher side-effects noted earlier in the event a user accidentally triggers the word filter – i.e., having to call a supervisor, having to re-boot the system, etc.

In all instances Bradshaw is quite clear that it is a "blocking" routine, and there is no circumventing or bypassing the security:

> Col 3, ll. 55+: "disabling" of the system must be done by a supervisory person
> Col. 4, ll. 10+: "...it also provides opportunities for a supervisor to intervene and provide corrective action..."
> Col. 6, ll. 50+: "...the blocking routine is designed to prevent any further use of the computer system by a user unless a supervisor intervenes to deactivate X-stop, preferably by entering a password.

Finally Applicant notes that the Examiner has selectively excerpted passages from Bradshaw without considering what relevance they have to the present invention. In particular, the Bradshaw reference actually shows four separate routines for monitoring a computer. There is a "keyboard monitor sentinel," a "mouse monitor sentinel," a "clipboard monitor sentinel" and a "winsock monitor sentinel." These are

shown generally in FIG. 1, and the flowcharts for each are given generally at FIGs. 3, 4, 5 and 6 respectively.

What these figures show is that the bulk of the language excerpted by the Examiner from Bradshaw pertains to the "keyboard" sentinel discussed at col. 8, l. 24 – col. 9, l. 54. This routine is monitoring words as they are entered on a keyboard by a user. Even if the supervisor intervenes, it does not cause an "*...email message* to be *transmitted* by the computing system *to an intended recipient*." It would merely allow the text to be *entered* into a document from the keyboard buffer. The fact that this routine does not check an *entire* "email message" as set out in the claims, as is evident from the Example 1 given at the end of the specification col. 11, ll. 27 – 31.

> The user is in a word processing application and types "mukky." The keyboard sentinel detects the typing of the prohibited word and blocks the system.

The only facility in fact for checking electronic documents (emails) in Bradshaw is discussed at col. 7, l. 8 – 38, where it indicates, again, that a *supervisor* can *manually* select to "block" email. *See e.g.* ll. 19+:

> Selecting "Block" from the main menu bar presents a pull-down menu with the choices "Block Server," "Block E-mail" and "Foul Language".

Bradshaw makes a passing reference to the fact that the sentinels *could* be expanded to check content of emails (see col. 12, ll. 46 – 49), but he certainly makes no mention of how such would be done, nor does he give any indication that an author would have a facility for bypassing such sentinel at his/her own discretion.

Like Cohen, Bradshaw does not teach or suggest the present claims, because the last thing it wants to do is be informative or useful to authors of documents. In fact, it openly suggests that it is preferable to discourage users from attempting to learn the appropriate words that might trigger the filters. See e.g. col. 9, ll. 11+:

> It was found that a blocking system that merely prevents use of certain words and use less drastic blocking techniques induce the use to experiment with various words and their forms, trying to find one that isn't blocked.

Thus it plainly teaches away from the present invention, which is intended to facilitate and assist authors to use appropriate language in their communications.

Finally the Applicant submits that the combination of Cohen and Bradshaw is inappropriate because the Examiner is simply selecting elements from different

references without consideration of the underlying requirements and strictures of the embodiments shown therein. As noted, Cohen clearly does not contemplate allowing users to bypass the filter.

The Examiner's brief conclusory citation of the "benefit" of this combination (see page 6) is nothing more than a re-hash of discussions taken from the *present* disclosure. This is clearly improper hindsight reconstruction of the claim, a methodology that is still unacceptable under current obviousness standards. Thus the Examiner's suggestion that Cohen would consider some kind of optional override (as argued to exist in Bradshaw) runs completely counter to the teachings of such reference.

For these reasons Applicants submit that the rejection of claim 83 based on Cohen and Bradshaw is not sustainable.

Applicants submit that the same rationale should apply for independent claim 96. Dependent claims 85 – 87 and 92 should be allowable for at least the same reasons.

2. Discussion for claims 88, 89 and 97 (depending from claims 83, 96 respectively) as being further unpatentable under § 103 in light of the Cohen/Bradshaw combination taken with Ishikawa (U.S. Patent No 5,812,863)

Claim 88 depends from claim 83, and as such should be allowable for at least the same reason as the latter.

With respect to dependent claims 89 and 97: again, each depends in some fashion from claim 83, and as such should be allowable for at least the same reason as the latter. Furthermore with respect to claims 89 and 97, these are submitted to distinguish over the claimed combination for the reason that Ishikawa does not show *separate* files for dictionaries; a single dictionary file is used which contains words with multi-value codings. To wit, claim 89 states:

> ....The method of claim 84, wherein said language filter *includes a second dictionary* with foreign language words *which second dictionary is part of a second electronic file which is separate from a first electronic file* used for said first set of words and can be considered separately from said first electronic file

Claim 97 is similarly worded.

The Examiner believes that Ishikawa uses two separate dictionaries. However it can be seen in col. 4, l. 48 that Ishikawa's only reference to a separate file is in connection with a "supplemental" dictionary which is *added* to the main dictionary for detecting misspellings. The implication is clear that only a single dictionary is ever consulted during operation of the Ishikawa system.

In contrast, the embodiment of claims 89, 97 cover a form of modular dictionary that makes the system more flexible. These two separate files for the two separate dictionaries can be considered separately. The Examiner's most recent comment seems to suggest that a *single* electronic file in Ishikawa *can be considered* as two files when the composition is changed (i.e. from Dictionary 1 to Dictionary 1 + Dictionary 2). There is in fact no suggestion in Ishikawa, however, that the system would ever consider a first file composed of Dictionary 1, and *then* a second file composed of Dictionary 1 + Dictionary 2 to check content of an email. The discussion referenced by the Examiner in Ishikawa is at best an either/or situation; it never would consider two files as noted in the claims at issue here.

3. Discussion for independent claim 98 (and claim 99 depending therefrom) and claims 90, 91, 93 (depending from claim 83) rejected as unpatentable under § 103 in light of Cohen/Bradshaw taken with Russell-Falla et al. (U.S. Patent No 6,671,162)

Claims 90, 91 depend from claim 83, and as such should be allowable for at least the same reason as the latter. Furthermore they should be allowable for the additional reasons that the prior art cited by the Examiner is inapposite. These claims recite:

> 90. The method of claim 83, wherein an author is alerted during step (d) only if a sensitivity threshold specified by the author is exceeded.
>
> 91. The method of claim 83, wherein said sensitivity threshold is specified as a numerical value ranging from 1 to 10.

The section cited by the Examiner against these claims is from Russell-Falla at c. 5, ll. 34 – 51; here is what it states:

Turning now to operation of the program from the end-user's perspective, again referring to FIG. **1**, the user interacts with a conventional web browser program, by providing user input **50**. Examples of well-known web-browser programs include Microsoft Internet Explorer and Netscape. The browser displays information through the browser display or window **52**, such as a conventional PC monitor screen. When the user launches the browser program, the user logs-in for present purposes by providing a password at step **54**. The user I.D. and password are used to look up applicable threshold values in step **56**.

In general, threshold values are used to influence the decision of whether or not a particular digital dataset should be deemed to contain the selected category of information content. In the example at hand, threshold values are used in the determination of whether or not any particular web page should be blocked or, conversely, displayed to the user. The software can simply select a default threshold value that is thought to be reasonable for screening pornography from the average user. In a preferred embodiment, the software includes means for a parent, guardian or other administrator to set up one or more user accounts and select appropriate threshold values for each user. Typically, these will be based on the user's age, maturity, level of experience and the administrator's good judgment. The interface can be relatively simple, calling for a selection of a screening level—such as low, medium and high—or user age groups. The software can then translate these selections into corresponding rating numbers.

The Examiner, in the most recent Office Action argues that this part of the disclosure should be interpreted as follows:

> However, Russell-Falla teaches wherein an author is alerted only if a sensitivity threshold specified by the author is exceeded (C.5.lines 34-51, abstract). The Examiner takes Official notice that a sensitivity threshold can

This statement is completely unsupported by the section of Russell-Falla above cited by the Examiner. The citation mentions setting a threshold on a browser, not on the web page in question. The reference makes no mention of these being thresholds being used by an author of an email message; they are thresholds being used by a web *surfer* looking at web pages.

The interpretation of Russel-Falla in which a web surfer could also be a web page author is clearly not reasonable, and the Office Action makes no effort to defend this logic. Moreover even if it were true, it still does not teach or suggest that the language filter is associated with the email message as set out in claim 83/90, allowing the author to control the content of the email message. Russell-Falla merely allows the browser to control whether and what parts of the web page they see after the latter is already created.

Consequently reconsideration is requested for claims 90 and 91.

Concerning independent claim 93; this claim should be allowable for at least the same reasons as claim 83 based on the distinctions over Cohen and Bradshaw. Moreover Applicant incorporates by reference the arguments already set forth against the Russel-Falla reference. It does not teach or suggest the limitation of claim 93:

> ....setting a sensitivity threshold provided by the author to also be used in connection with checking appropriateness of content included in the email message

The Examiner cites col. 5, ll. 33+ of Russel – Falla. Again, see above; the reference says nothing about allowing *authors* to control the content of their messages.

Accordingly this claim is believed to be distinguishable over the cited combination, which does not permit the author of the document to adjust a sensitivity threshold.

Dependent claims 98 – 99 should be allowable for essentially the same reasons as claim 93.

4. **Discussion of rejection of independent claim 94 (and claim 95 depending therefrom) and independent claims 100, 102 (and claims 101, 103 depending from these claims respectively) as unpatentable under § 103 in light of Cohen/Bradshaw taken with Rayson et al. (U.S. Patent No 5,761,689)**

Independent claims 94 – 95 should be allowable for the same reasons as claim 83 previously discussed.

Applicant disagrees with the argument that one skilled in the art would reasonably combine Rayson with Cohen: the former is directed to a word processing tool. The Examiner merely states that they are both filtering tools; this may be true, but

they are dramatically different tools and there is no suggestion anywhere that they should or could be combined.

Cohen is primarily an email filter; thus in Cohen the message is checked only *after* it is completely composed. There is no mention whatsoever of what the message composition program looks like, or how it could be modified to accommodate the change now suggested by the Examiner. In other words, Cohen only shows filtering a message as it goes through the last part of a message router. There is no suggestion or explanation of how one could incorporate the filtering aspects at step 80 (Fig. 1) let alone incorporate the immediately after in time related features of Rayson. Thus the Examiner is trying to modify Cohen with characteristics that are not supportable.

Independent claim 100 should be allowable for the same reasons as claims 83 and 94 – 95 previously discussed. Dependent claim 101 should be allowable for at least the same reasons.

Independent claim 102 should be allowable for the same reasons as claims 83, 94 – 95 and 100 previously discussed, and for the reasons set out in the prior response.

Dependent claim 103 should be allowable for at least the same reasons.

IX. CLAIMS

A copy of the claims involved in the present appeal is attached hereto as Appendix A.

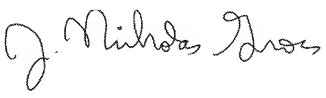
X. EVIDENCE

No additional evidence pursuant to §§ 1.130, 1.131 or 1.132 or entered by or relied upon by the Examiner is being submitted.

XI. RELATED PROCEEDINGS

No related proceedings are referenced herein, nor are copies of decisions in related proceedings being provided, as there are none. Accordingly, no Appendix is included.

Respectfully submitted,



J. Nicholas Gross
Registration No. 34,175
Attorney for Applicant(s)

June 9, 2008
2030 Addison Street
Suite 610
Berkeley, CA 94704
510-540-6300
510-540-6315 (fax)

APPENDIX A

1 – 82 (previously canceled)

83. (Previously amended) A method of permitting an author of an electronic mail (email) message to check text content using an electronic text editor program operating on a computing system, the method comprising:

(a) selecting a language filter for checking words in the email message, which language filter includes a first set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; and

(b) receiving input words entered by the author as text for the email message;

(c) inspecting said input words to determine if they fall within said language filter;

(d) alerting the author when one or more of said input words fall within said language filter;

(e) permitting the author to change words within the email message after step (d) and before the email message is transmitted to said intended recipient; and

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter.

84. (Original) The method of claim 83, wherein said language filter includes obscene, vulgar and/or racist words found in a first pre-programmed dictionary created without input from the author.

85. (Original) The method of claim 83, wherein step (d) includes providing a highlighting of any words which are determined to fall within said language filter along with an accompanying visual warning.

86. (Previously amended) The method of claim 83 further including a step: identifying a language filter to the author which was triggered during step (d).

87. (Original) The method of claim 83, further including a step (f): checking one or more additional electronic email message files according to steps (a) through (d).

88. (Original) The method of claim 83, further including a step (f): checking spelling of the email message.

89. (Previously Amended) The method of claim 84, wherein said language filter includes a second dictionary with foreign language words which second dictionary is part of a second electronic file which is separate from a first electronic file used for said first set of words and can be considered separately from said first electronic file.

90. (Original) The method of claim 83, wherein an author is alerted during step (d) only if a sensitivity threshold specified by the author is exceeded.

91. (Original) The method of claim 83, wherein said sensitivity threshold is specified as a numerical value ranging from 1 to 10.

92. (Original) The method of claim 83, wherein steps (a) through (e) are implemented as a software routine in machine readable form executable by a personal computer.

93. (Previously amended) A method of permitting an author of an electronic mail (email) message to check text content using an electronic text editor program operating on a computing system, the method comprising:

(a) selecting a language filter for checking words in the email message, which language filter can be configured to control dissemination of content to an intended recipient of the email message; and

(b) setting a sensitivity threshold provided by the author to also be used in connection with checking appropriateness of content included in the email message;

(c) retrieving input words entered by the author as text for the email message;

(d) inspecting said input words to determine if they fall within said language filter;

(e) providing a warning to the author if an input word falls within said language filter and said sensitivity threshold is exceeded;

(f) permitting the author to change words within the email message after a warning is made and before the email message is transmitted to said intended recipient; and

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter.

94. (Previously amended) A method of checking text content of an email message using an electronic text editor program operating on a computing system, the method comprising:

(a) selecting a language filter for checking words in the email message, which language filter includes a set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; and

(b) receiving an input word entered by the author as text for the email message;

(c) inspecting said input word substantially immediate in time after it is entered to determine if it falls within said language filter;

(d) providing a warning to the author when said input word is determined to fall within said language filter ;

(e) permitting the author to change said input word within the email message after a warning is made and before the email message is transmitted to said intended recipient; and

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if said input word falls within said language filter.

95. (Previously amended) A method of checking text content of an email message using an electronic text editor program operating on a computing system, the method comprising:

(a) selecting a language filter for checking words in the email message, which language filter includes a set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; and

(b) receiving input words entered by the author as text for the email message;

(c) inspecting said input words during idle periods when the author is not interacting with said electronic text editor program to determine if such input words fall within said language filter;

(d) providing a warning to the author when one or more of said input words are determined to fall within said language filter;

(e) permitting the author to change words within the email message after a warning is made and before the email message is transmitted to said intended recipient; and

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter.

96. (Previously amended) A computer program for checking text content of an email message using an electronic text editor program operating on a computing system, comprising:

a language filter for checking words in the email message, which language filter is an electronic dictionary which includes a set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; and

a content checking routine which is adapted for:

i) receiving input words entered by the author as text for the email message;

ii) inspecting said input words to determine if they fall within said language filter;

iii) generating an alert to the author when ~~on~~ one or more of said input words fall within said language filter;

iv) permitting the author to change words within the email message after an alert is generated and before the email message is transmitted to said intended recipient; and

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter.

97. (Previously amended) The computer program of claim 96, wherein said language filter includes at least a first dictionary located in a first electronic file and a second separate dictionary located in a separate second electronic file, and said alert includes an indication of which of said of said first dictionary or said second dictionary was triggered by said alert.

98. (Previously amended) A computer program for permitting an author of an electronic mail (email) message to check text content, comprising:

a language filter for checking words in the email message, which language filter can be configured to control dissemination of content to an intended recipient of the email message; and

a content checking routine which is adapted for:

i) setting a sensitivity threshold provided by the author to also be used in connection with checking appropriateness of content included in the email message;

ii) retrieving input words entered by the author as text for the email message;

iii) inspecting said input words to determine if they fall within said language filter;

vi) providing a warning to the author if an input word falls within said language filter and said sensitivity threshold is exceeded;

vii) permitting the author to change words within the email message after a warning is made and before the email message is transmitted to said intended recipient; and

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter.

99. (Original) The computer program of claim 97, wherein said sensitivity threshold is used during a check of individual words in said language filter.

100. (Previously amended) A computer program operating on a computing system for checking text content of an email message comprising:

a language filter for checking words in the email message, which language filter includes a set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; and

a content checking routine adapted for:

i) receiving an input word entered by the author as text for the email message;

ii) inspecting said input word substantially immediate in time after it is entered to determine if it falls within said language filter;

v) providing a warning to the author when said input word is determined to fall within said language filter ;

vi) permitting the author to change said input word within the email message after a warning is made and before the email message is transmitted to said intended recipient; and

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter.

101. (Original) The computer program of claim 100, wherein said input word is checked before the author has entered another input word.

102. (Previously amended) A computer program operating on a computing system for checking text content of an email message comprising:

a language filter for checking words in the email message, which language filter includes a set of words that could be offensive and/or potentially inappropriate for use in connection with an intended recipient of the email message; and

a content checking routine adapted for:

i) receiving input words entered by the author as text for the email message;

ii) inspecting said input words during idle periods when the author is not interacting with said electronic text editor program to determine if such input words fall within said language filter;

v) providing a warning to the author when one or more of said input words are determined to fall within said language filter;

vi) permitting the author to change words within the email message after a warning is made and before the email message is transmitted to said intended recipient; and

wherein the author of the email message can cause the email message to be transmitted by the computing system to said intended recipient even if words in such email message still fall within said language filter.

103. (Original) The computer program of claim 102, wherein said input words are also checked for spelling during said idle periods.